(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

10/500983

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number
WO 03/058409 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP03/00075

(22) International Filing Date: 7 January 2003 (07.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 00 288.6 7 January 2002 (07.01.2002) DE

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS GMBH** [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRESSY, Philippe** [FR/FR]; 8, rue du Lancon, F-83190 Ollioules (FR). **LOISEL, Yann** [FR/FR]; Lotissement Le Revestin, Chemin des Severiers, F-13600 La Ciotat (FR).

(74) Agent: **DEGWERT, Hartmut**; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

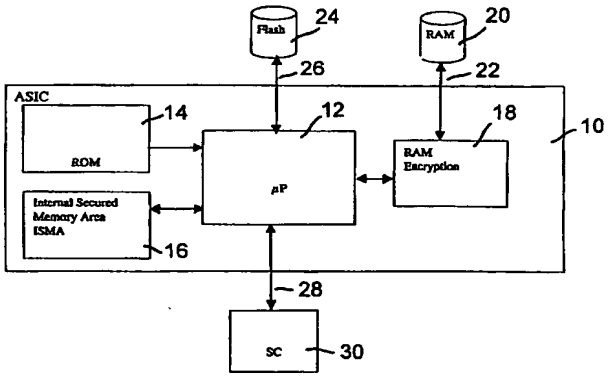
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTECTING A DEVICE AGAINST UNINTENDED USE IN A SECURE ENVIRONMENT



(57) Abstract: A method and device are disclosed for executing applications that involve secure transactions and/or conditional access to valuable contents and/or services. The device includes an integrated circuit that has a central processing unit, an internal memory, input/output connections for external memory and connection ports for an external interface circuit incorporated on a single chip. The internal memory includes a secured memory area accessible to the central processing unit only. The secret memory area contains a secret encryption key used for encryption of sensitive data stored in the external memory. Preferably, the chip includes a random number generator. A hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with the secret key, and the encrypted random number with its hash value are and stored in the external memory. As a result, the device has a chip that is uniquely paired with the external memory. Since the sensitive data and/or code are of such nature that proper execution of an application by the device will not be possible unless these data and/or code have been successfully decrypted, and the chip will not decrypt the data and/or code unless it has successfully checked its pairing with the external memory, the device is effectively protected from use with other than authentic contents of the external memory.

WO 03/058409 A2

Protecting a Device Against Unintended Use in a Secure Environment

Field of the Invention

The present invention relates to a method of protecting a device against unintended use in a secure environment and, in particular, in a conditional access environment. The invention also relates to a device for executing applications that involve conditional access to valuable contents and/or valuable services.

Background of the Invention

Examples of applications that involve secure transactions are electronic payment and banking; examples of applications that involve conditional access are Digital Pay TV, recording of Digital TV and Video on Demand. A device for executing such applications can be a module that is embedded in an environment such as a Set-Top-Box, a chip embedded on the motherboard of a Set-Top-Box, a Smart Card reader or a pluggable module such as a PC card that typically includes a Smart Card reader. While hardware components in the module ensure high performance for tasks such as descrambling of real time video streams, the Smart Card mainly has a security functionality. Application code is typically stored into an external memory of the device, such as a FLASH memory.

Conventionally, these devices rely on security that resides in the Smart Card. To the extent, however, that overall security depends on procedures contained in application code stored in external or even in internal memory of the device, the security functions of the Smart Card can be worked-around by replacement or modification of application code.

Summary of the Invention

The present invention provides a secure architecture for a device that executes applications under high requirements of security.

According to a first aspect of the invention, a method of protecting a device against unintended use in a secure environment is provided, where the device is adapted to execute applications that involve secure transactions and/or conditional access to valuable contents and/or services, and the device includes an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory, all incorporated on a single chip. The external memory and the chip are uniquely linked by encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory of the chip, the encrypted code and data being then stored in the external memory. Any use of the sensitive application code and data will be possible only after successful decryption with the secret key. Preferably, a random number and its hash value are also encrypted with the secret key and stored in the external memory. On each reset of the device, the encrypted random number and the hash value are decrypted with the secret key, and decryption of the encrypted sensitive code and data is only allowed if the decrypted hash value equals a hash value calculated from the decrypted random number. As a result, the chip and external memory are uniquely paired, i.e. the chip cannot be used with an external memory the sensitive contents of which have been altered or exchanged.

The invention also provides a device for executing applications that involve secure transactions and/or conditional access to valuable contents and/or services.

The device includes an integrated circuit that has a central processing unit, an internal memory and input/output connections for an external memory, all incorporated on a single chip. The internal memory includes a secured memory area accessible to the central processing unit only. The secured memory area contains a secret encryption key used for encryption of sensitive data stored in the external memory. Preferably, the chip includes a random number generator. A hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with the secret key, and the encrypted random number with its hash value are and stored in the external memory. As a result, the device has a chip that is uniquely paired with the external memory. Since the sensitive data and/or code are of such nature that proper execution of an application by the device will not be possible unless these data and/or code have been successfully decrypted, and the chip will not decrypt the data and/or code unless it has successfully checked its pairing with the external memory, the device is effectively protected from use with other than authentic contents of the external memory.

The secured memory area may contain authenticity verification data. The internal memory may also include a read only memory area containing mandatory authenticity verification code allowing an application to be executed only after successful verification of authenticity. Therefore, only authentic application code is executed by the device, and any replacement of application code attempting to circumvent safety functionality will not be successful.

As used herein, "authenticity" is understood in a broad sense. In the preferred embodiments of the invention, as defined in the appending claims, "authenticity" includes integrity, and any fraudulent modification of application code or sensitive data results in refusal by the device to execute the application.

In further preferred embodiments of the invention, as defined in the appending claims, any sensitive application code and data are never visible in the clear from outside of the device. Sensitive application code and data are stored in encrypted

form and decrypted within the device for execution of the application. By adding confidentiality to authenticity, an attack will be even more difficult, if not impossible, because the contents in memory, as visible from outside of the device, will not be intelligible.

According to a further aspect of the invention, any application code down-loaded into the device is signed with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of the key pair. In addition, any application code stored into the external memory is encrypted with a secret key that is stored in a secured memory area of the internal memory.

Short Description of Drawings

Further advantages and features of the invention will become apparent from the following description with reference to the appending drawings. In the drawings:

Fig. 1 is an overall schematic diagram of a device with a generic secure system architecture for a Conditional Access Module (CAM) and a Smart Card Reader (SCR);

Fig. 2A and 2B are diagrams illustrating different embodiments of procedures for preparing signed application code to be down-loaded into the device;

Fig. 3A to 3D are diagrams illustrating corresponding embodiments of signature verification procedures within the device;

Fig. 4A is a block diagram illustrating a procedure for preparing encrypted application code to be downloaded into the device;

Fig. 4B is a flow-chart illustrating decryption of the down-loaded application;

Fig. 5A and 5B are flow charts illustrating encryption and decryption of application code stored in external memory of the device;

Fig. 6 is a diagram illustrating a procedure of chip pairing whereby a chip is uniquely linked to contents in an external memory of the device;

Fig. 7 is a diagram illustrating a chip pairing verification procedure;

Fig. 8 is a diagram illustrating a first step of a chip personalization process; and

Fig. 9 is a diagram illustrating a second step of a chip personalization process;

Fig. 10 is a schematic representation of a variable assignment between external chip pins and internal chip signal lines; and

Fig. 11 is a block diagram of an intrusion detection arrangement.

Detailed Description of Preferred Embodiments

Overall Device Design

Referring now to Fig. 1, the device of the present invention includes an application specific integrated circuit (ASIC) that is generally designated at reference numeral 10. The ASIC 10 incorporates, on a single semiconductor chip, a number of components; among these components, the following are essential to the invention (although the ASIC will typically include other components):

- a microprocessor unit (μP) 12,
- a read only memory (ROM) 14 connected to μP 12,
- an internal secured memory area (ISMA) 16 also connected to μP 12.

Preferably, as shown in Fig. 1, the ASIC also includes a hardware encryption unit 18 connected to μP 12 and to an external random access memory (RAM) 20 via a

bi-directional interface 22, symbolized in Fig. 1 by a double arrow. In addition to external RAM 20, the device 10 has an external Flash memory 24 connected to µP 12 via a bi-directional interface 26 symbolized in Fig. 1 by a double arrow. The device 10 further includes a bi-directional interface 28 for connection to an external Smart Card (SC) 30.

In a specific embodiment, the device 10 incorporates conditional access (CA) functionality. Such a device is generally referred to as a CAM (Conditional Access Module) for use with a Set-Top-Box (STB) in a digital TV (DTV) environment. A CAM can be embedded within the STB, or it is a pluggable PC (PCMCIA) card fitting into a Common Interface (CI) slot of the STB, and incorporates a Smart Card Reader (SCR). Other embodiments of the device 10 include a SCR for use with a Personal Computer under high requirements of security.

Signed Down-Load

With reference to Fig. 2A, a first aspect of the invention is that any application to be executed by the device, at least to the extent it involves sensitive transactions, is checked for authenticity and integrity. Generally stated, the application code is signed with a key, and execution of the application by the device is subject to a positive verification of the signature. Various embodiments of this concept are proposed herein.

In each embodiment, a hash function obtains a hash value from the application code. The hash value is encrypted with a private key of a key pair. The public key of the key pair is stored in the memory of the device and, being a public key not specific to a particular customer, it can be stored in ROM 14.

In a first embodiment, as seen in Fig. 2A, the key pair includes a private key referred to as "SignDownPrK"; in the first embodiment, this SignDownPrK is a

Secure Architecture Designer's private key (SADPrivateKey). The corresponding public key (SADPublicKey) is stored in ROM 14. In Fig. 2A, "C" is application code in the clear, intended to be downloaded into the device. Further, a signature "D" in Fig. 2A is the hash value of the application code as encrypted with the private key.

With reference to Fig. 3A, where like symbols as in Fig. 2A are used, C and D are received in the device. A hash value C' is obtained from C with a hash function read from ROM 14. D is decrypted to D' with the public key (SADPublicKey) read from ROM 14 using an algorithm stored in ROM 14. If C' equals D', the application code C is valid and enabled for execution by the device; otherwise, the application code C is erased. After validation of application code C, it is loaded into RAM 20, preferably after encryption in RAM encryption interface 18. The microprocessor 12 will have access to application code in RAM 20 without significant loss of performance even though it is encrypted and must be decrypted by RAM encryption interface 18 prior to its execution, the RAM encryption interface being implemented in hardware. Alternatively or in addition, the validated application code is permanently stored, e.g. in external memory 24, but preferably in encrypted form.

In a second embodiment, a customer's private key (CustomerPrivateKey) is used for encryption of the hash value of application code C, rather than SADPrivateKey.

As used herein, "customer" means an organisation that offers valuable services and contents to end-users. Typically, the "customer" would purchase the device of the present invention, or at least the ASIC 10, from the Secured Architecture Designer (SAD) or a contract manufacturer of the SAD, and supply the device to an end-user in a finished product.

Now, in a first variant of this second embodiment, the public part of a customer key pair is stored in internal secured memory area (ISMA) 16. As seen in Fig. 3B,

that public key is read from ISMA 16 and used for verification of signature D. All other steps are the same as those in Fig. 3A.

In a second variant of the second embodiment, the Secure Architecture Designer's public key (SADPublicKey) is stored in ROM 14, and the customer's public key is signed with the SAD Private Key and can, therefore, be safely stored in the external memory 24. With reference to Fig. 3C, the CustomerPublicKey is first retrieved by decrypting, with SADPublicKey read from ROM 14, the encrypted customer's public key read from external memory 24, and then signature D is verified as in Fig. 3B.

In a third variant of the second embodiment, and with reference to Fig. 2B, a protected version of the CustomerPublicKey is down-loaded with the application code C into the device, so that the CustomerPublicKey will never be available in the external memory 24. Specifically, a hash value of CustomerPublic key is encrypted with SADPrivateKey to "F" and downloaded into the device along with CustomerPublicKey "E". With reference to Fig. 3D, verification of the application's signature is preceded by a verification of CustomerPublicKey. Downloaded CustomerPublicKey E is hashed and the hash value E' is compared with the result F' of decrypting, with SADPublicKey, the downloaded encrypted hash value F of CustomerPublicKey. If E' equals F', the verification proceeds to the verification of the application's signature D, as in Fig. 3C; otherwise, the application code C is rejected.

Except for the third variant of the second embodiment of the signed download method, the downloaded application code can be stored in the external memory 24 of the device.

Encrypted Down-Load

While the procedures disclosed so far ensure authenticity and integrity of an application to be executed by the device, a further proposal of the invention is to add confidentiality. As far as downloading of an application is concerned, confidentiality is achieved by encrypting the application code prior to its download.

With reference to Fig. 4, application code to be downloaded into the device is encrypted to "A" with SADSecretKey, a secure architecture designer's symmetric key. A hash value of the application is encrypted to "B" with SADSecretKey. The encrypted application and its encrypted hash value, A and B, are now downloaded into the device. With reference to Fig. 4B, A and B are decrypted to A' ad B', respectively, using SADSecretKey read from the secured memory area 16. A' (the application code in the clear, if correctly decrypted) is hashed to B'', and B'' is compared with B' (the application's code hash value, if correctly decrypted). If B'' equals B', the down-loaded and decrypted application code A' is validated; otherwise, A' is rejected.

The validated application code can now be used, e.g. it can be permanently stored in external memory 24 but, in the preferred embodiment, it will be encrypted before it is stored.

External Memory Encryption

In the scenario depicted in Fig. 5A, application code is available from RAM 20 after a signed and/or encrypted download, for example. Being a validated application, it can be stored in permanent external memory 24, but preferably not in the clear as far as sensitive software code and data are concerned.

Initially, the ASIC thus selects sensitive code and data to be encrypted. Depending on the required level of security and flexibility, an encryption key KF is used directly or a derived key is used. As a first option, KF is the SADSecretKey read from secured memory area 16. The selected sensitive code and data are encrypted

with that key and stored in external memory 24, along with other, non-sensitive code and data.

As a second option, KF is the ChipSecretKey, also read from the secured memory area.

As a third option, a random number "RN" is used as the encryption key, KF=RN, RN is encrypted with SADSecretKey read from the secured memory area 16, and the encrypted random number is stored in external memory 24 as "RNEnc".

As a fourth option, the sensitive code and data are compressed by the ASIC prior to encryption.

As a fifth option, a secret chip random number "ChipRandomNumber" is fetched from the secured memory area 16. The ChipRandomNumber and a hash value thereof are encrypted with encryption key KF to X and Y, respectively. The encrypted random number X and its encrypted hash value Y are stored in external memory 24, along with the encrypted sensitive code and data and other, non-sensitive code and data.

As a sixth option, the sensitive code and data are hashed and encrypted with key KF. The result EncH is stored in external memory 24 along with the encrypted sensitive code and data and other, non-sensitive code and data.

With reference now to Fig. 5B, and according to the respective option among options 1 to 6, the appropriate key KF must be determined. With key KF, the encrypted contents of the external memory 24 are decrypted and can be used, e.g. for execution of an application.

If it is option 1, KF is SADSecretKey, as read from the secured memory area 16.

If it is option 2, KF is ChipSecretKey, as read from the secured memory area 16.

If it is option 3, KF is obtained by decrypting the encrypted random number RNEnc read from the external memory 24 with the SADSecretKey read from secured memory area 16.

With option 4, the decrypted contents of external memory 24 are decompressed before they are used.

Option 5 requires an integrity check for the contents of external memory 24. The encrypted random number X and its encrypted hash value Y are decrypted to X' and Y' with KF, the decrypted random number X' is hashed to Y'' and the result is compared with the decrypted hash value Y'. If Y'' equals Y', the content of external memory 24 is validated; otherwise, it is rejected.

With option 6, integrity of the encrypted sensitive code and data is checked. Specifically, the encrypted hash value EncH is read from external memory 24 and decrypted to H with key KF. A hash value H' is calculated from the decrypted sensitive code and data. Only if both hash values H and H' are equal, the decrypted sensitive code and data are validated.

It is understood that options 4, 5 and 6 are not mutually exclusive and can be used separately or jointly with any of options 1 to 3.

Chip – External Memory Pairing

To further protect the device, the invention proposes to uniquely link the chip of the device with the contents of the external memory 24 (External Memory – ASIC Pairing).

With reference to Fig. 6, sensitive application code and data are identified within external memory 24 and encrypted to "I" with secret chip key "ChipSecretKey"

read from the secured memory area 16, and I is stored in external memory 24. The sensitive application code and data are such that proper execution of the application is impossible without successfully decrypting the code and data. The random number generator within the chip of the device generates a random number "RNG" which is hashed to "K". The random number RNG and its hash value K are encrypted to "J" with "ChipSecretKey", and J is also stored in external memory 24. The chip is now uniquely linked to the external memory 24.

With reference to Fig. 7, the chip verifies its pairing with external memory 24 at least after each reset of the device. Specifically, J (the encrypted random number and its hash value) is read from external memory and decrypted with "ChipSecretKey" to "W" and "Z". The calculated hash value of W, " Z' ", is compared with the decrypted hash value Z of random number W. Only if Z and Z' are equal, pairing is confirmed and the sensitive application code and data can be retrieved from I read from the external memory by decrypting I; otherwise, some appropriate action is taken to prevent unintended use of the device.

Chip Personalization

Immediately after its manufacturing, the chip of the device only has a basic functionality by software and data stored in ROM 14. Software initially stored in ROM 14 includes a boot procedure, a download routine, a cryptography library and other basic functions. Data initially stored in ROM 14 includes a Serial Number, the SADPublicKey and a hash value over the ROM content. The secure memory area 16 will be empty, and the chip will be without defence against unintended use.

Therefore, according to a further proposal of the invention, the chip is personalized before it is delivered to a customer.

With reference to Fig. 8, a first level personalization of the chip includes storing a secret symmetric personalization key "PersoSecretKey" in the secured memory area 16 (ISMA). An internal information field within secured memory area 16, "ISMAInfo", is updated to indicate that PersoSecretKey is available. A hash value ISMAContentHash over the content of the secured memory area 16 is calculated and also stored in the secured memory area.

The chip can now be shipped to a customer where a second level personalization will be made before delivery of the chip to an end-user within a finished product. Alternatively, the second level personalization is already performed by the Secure Architecture Designer (SAD) before the chip is shipped to the customer or end-user.

With reference to Fig. 9, a second level personalization is illustrated which can be performed by the Secure Architecture Designer or by a customer. The Secure Architecture Designer provides a particular personalization application the purpose of which is to write into the device sensitive data and information pertaining to the intended use of the device. For download into the device, the personalization application "PersoAppli" is encrypted with the secret symmetric personalization key "PersoSecretKey", and a hash value of the application code is calculated and signed with a Secure Architecture Designer's private key "SADPrivateKey". Alternatively, both the application code and its hash value signed with "SADPrivateKey" are encrypted with the secret symmetric key "PersoSecretKey" and downloaded into the device. The device will be able to decrypt the encrypted application code with "PersoSecretKey" read from the secured memory area 16, and to check the signature of its hash value with "SADPublicKey" read from ROM 14. After execution of the personalization application by the device, all sensitive data and information have been written into the device, "ISMAInfo" is updated, a new "ISMAContentHash is computed and stored, "PersoSecretKey" is erased and the application is also erased.

Variable Terminal Assignment

As should be clear from the preceding description, the method of the present invention requires access to protected parts of the chip in order to initiate the chip with basic confidential and sensitive data and, in particular, those written into secured memory area 16. In order to protect the chip against non-authorized access to sensitive parts, the invention proposes a secret access channel that must be used to access sensitive parts of the device.

With reference to Fig. 10, the ASIC includes a silicon core body 30 with a number of internal chip connections 32 and a number of external terminals 34 (pins or pads). Within the package 36 of the ASIC, an internal row of parallel conductor lines 38 permits to connect any of the internal chip connections to any of the external terminals 34. At least some of the assignments between internal chip connections 32 and external terminals 34 are variable and are materialised by selectively operated switches such as switches 40, 42 in Fig. 10. In order to establish a secret access channel, selective ones of the switches 40, 42 are closed and, after use of the secret channel such as for the above personalization steps, can be opened and left open.

Intrusion Detection

Whenever an intrusion of any kind is detected, appropriate steps are taken to prevent unintended use of the device. Typically, the contents of the secured memory area 16 are erased.

With reference to Fig. 11, the ASIC 10 includes an intrusion detector 50. In the proposed embodiment, the secured memory area 16 within ASIC 10 is a RAM that needs a continuous power supply to maintain information stored therein. Secured memory area 16 (RAM) receives power from an external battery 52 connected to external supply and ground terminals of the ASIC. A controllable switch 54 is inserted in the supply path of memory area 16. Switch 54 is normally

closed and is controlled by intrusion detector 50. Intrusion detector 50 has a number of inputs connected to corresponding monitoring devices. One such monitor device can be a photo-transistor 56 that would detect any light penetrating into the chip package upon physical attack of its envelope. Another monitor device can be a temperature sensor 58 that would detect any abnormal temperature. The intrusion detector 50 is also connected to the main device power supply and to ground and would detect any abnormal supply voltage or power consumption. Yet another input to intrusion detector 50 is connected to the system clock generator 60 and would detect any abnormal clock rate. A watch-dog 62 connected to a further input of intrusion detector 50 would detect any abnormal absence of activity from microprocessor 12 within a given time. Any failure of an integrity, authenticity or signature check is also signalled from microprocessor 12 to the intrusion detector 50.

Each abnormal condition signalled to the intrusion detector 50 by any of the monitor devices would cause the switch 54 to be opened, and all information within the secured memory area 16 would be erased.

Claims

1. A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve conditional access to at least one of valuable contents and services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, characterized in that said external memory and said chip are uniquely linked by encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory, the encrypted code and data being then stored in said external memory.

2. The method of claim 1, wherein a random number and a hash value of the random number are also encrypted with said secret key and stored in the external memory, the encrypted random number and hash value are decrypted with the secret key at least on each reset of the device, and decryption of the encrypted sensitive code and data are only allowed if the decrypted hash value equals a hash value calculated from the decrypted random number.

3. The method of claim 1 or claim 2, characterized in that application code down-loaded into the device is signed with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair.

4. The method of claim 3, wherein the signature is generated by obtaining a hash value from said application code and encrypting the hash value with the private key.

5. The method of claim 3 or claim 4, wherein the public key of said key pair is stored in an internal read only memory of the device.

6. The method of claim 3 or claim 4, wherein the public key of said key pair is stored in an internal secured memory area of the device.

7. The method of claim 3 or claim 4, wherein a secure architecture designer's public key is stored in an internal read only memory of the device, a customer's public key is signed with the designer's private key and stored in the external memory, the customer's public key is retrieved by decrypting with the designer's public key read from the read only memory, the encrypted customer's public key read from the external memory, and the signature is verified.

8. The method of claim 3 or claim 4, wherein the public key of said key pair is downloaded with the signed application code and a hash value of the public key is encrypted with a private key the corresponding public key of which is stored in internal read only memory of the device, and the encrypted hash value is also downloaded to the device.

9. The method of any of claims 1 to 8, wherein the application code is downloaded into the device, encrypted with the secret key and stored in the external memory.

10. A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve secure transactions and/or conditional access to valuable contents and/or services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip;

characterized in that

a) any application code down-loaded into the device is signed with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair;

b) said external memory and said chip are uniquely linked by encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory and storing the encrypted code and data in the external memory;

c) a random number and a hash value of the random number are also encrypted with said secret key and stored in the external memory;

d) on each reset of the device, the encrypted random number and hash value are decrypted with the secret key, and decryption of the encrypted sensitive code and data are only allowed if the decrypted hash value equals a hash value calculated from the decrypted random number.

11. A method according to any of the preceding claims, characterized in that, after manufacturing of the chip and prior to delivery to a customer, a secret access channel is established to write a secret personalization key into the secure memory area.

12. The method of claim 11, wherein the content of the secure memory area is protected by calculating a hash value of the secure memory area content and writing the hash value into the secure memory area.

13. The method of claim 11 or 12, wherein a personalization application is signed with a Secure Architecture Designer's private key and then encrypted with the secret personalization key, the personalization application is loaded into the device and decrypted with the secret personalization key, the signature of the personalization application is checked with the Secure Architecture Designer's public key, and the personalization application is executed to write sensitive personalization data into the secure memory area.

14. The method of claim 11 or 12, wherein a personalization application is encrypted with a secret symmetric key stored in a secured memory area of the device, a hash value of the personalization application is signed with a Secure Architecture Designer's private key, the encrypted personalization application and the signed hash value are loaded into the device, the personalization application is decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

15. The method of claim 11 or 12, wherein a personalization application and a hash value of the personalization application signed with a Secure Architecture Designer's private key are encrypted with a secret symmetric key stored in a secured memory area of the device, the encrypted personalization application and signed hash value are loaded into the device, the personalization application and signed hash value are decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

16. A method according to any of the preceding claims, characterized in that the external memory includes a RAM and the chip has a bi-directional encryption/decryption hardware interface ensuring high performance and yet encrypted exchange of data between the chip and the RAM.

17. A device for executing applications that involve conditional access to at least one of valuable contents and services, including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip,

characterized in that the internal memory includes a secured memory area accessible to the central processing unit only and containing a secret encryption key used for encryption of sensitive data stored in the external memory.

18. The device according to claim 17, wherein said chip includes a random number generator.

19. The device of claim 18, wherein a hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with said secret key, and the encrypted random number with its hash value are and stored in the external memory.

20. The device according to any of claims 17 to 19, wherein encryption is limited to sensitive application code and data.

21. The device according to any of claims 17 to 20, wherein said external memory is a flash memory.

22. The device according to any of claims 17 to 21, wherein a secret device key associated with each particular device is stored in said secured memory area, sensitive data are encrypted with said secret device key, the encrypted sensitive data are stored in the external memory and the encrypted sensitive data in the external memory are decrypted and verified at least at each reset of the device.

23. The device according to any of claims 17 to 22, wherein said secured memory area includes a signature verification public key used for verification of a signature attached to application code to be executed by the device.

24. The device according to any of claims 17 to 22, wherein application code to be executed by the device is stored in said external memory with an attached signature and with a signature verification key encrypted with a private key, a corresponding public key being stored in the read only memory of the device.

25. The device of claim 23 or claim 24, wherein an encrypted hash value of sensitive application code and data is added to application code stored in said external memory.

26. The device according to any of claims 17 to 25, wherein said secured memory area includes personalization data pertaining to an intended use, an intended customer and an intended configuration of the device.

27. The device according to claim 26, wherein said external memory includes an application code storage into which application code can be loaded subject to compliance with said personalization data.

28. The device according to any of claims 17 to 27, wherein said secured memory area is loaded with at least one secret key and a hash value of the content of the secured memory area prior to delivery of the chip to a customer.

29. The device according to any of claims 17 to 28, wherein the chip comprises intrusion detection means for, in response to a detected intrusion, erasing at least essential parts of said secured memory area.

30. The device according to any of claims 17 to 29, wherein the chip includes a watch-dog and the chip is reset or at least essential parts of said secured memory area are erased when no activity is detected by the watch-dog within a predetermined time.

31. The device according to any of claims 17 to 30, wherein the chip includes a clock monitor and any abnormal variation of the chip clock rate causes the chip to reset or at least essential parts of said secured memory area to be erased.

32. The device according to any of claims 17 to 31, wherein said chip has outer connection terminals that are variably assigned to internal connections, and a secret terminal assignment is used to supply secret keys and/or procedures to said memory.

33. The device of any of claims 17 to 32, comprising a read only memory area that contains mandatory authenticity verification code allowing an application to be executed by the device only after successful verification of authenticity, the secret memory area also containing authenticity verification data, and wherein said authenticity verification code is contained in a boot procedure.

34. The device of claim 33, wherein said internal memory includes a ROM and at least part of said authenticity verification data is obtained by applying a predetermined hash function to at least a predefined part of the ROM content.

35. The device of claim 34, wherein said authenticity verification code applies said predetermined hash function to said predefined part of the ROM content and compares the hash value with a corresponding part of the authenticity verification data.

36. The device according to any of claims 33 to 35, wherein said at least part of said authenticity verification data is obtained by applying a predetermined hash function to the content of the secured memory area.

37. The device of claim 36, wherein said authenticity verification code applies said predetermined hash function to the content of the secured memory area and compares the hash value with the corresponding part of the authenticity verification data.

Figure 1

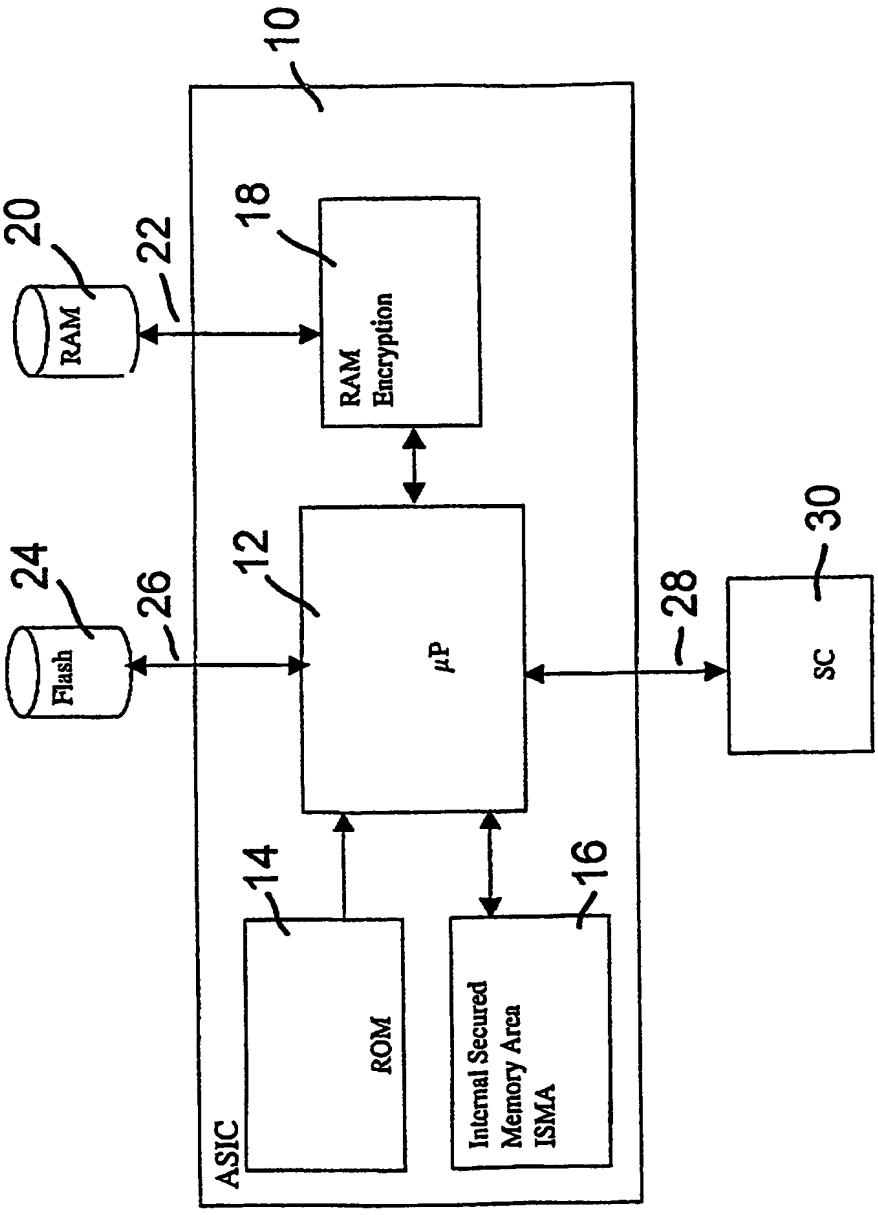

10
20
22
RAM
18
RAM Encryption
24
26
Flash
12
µP
28
30
SC
14
ROM
16
Internal Secured Memory Area ISMA
ASIC

Figure 2A

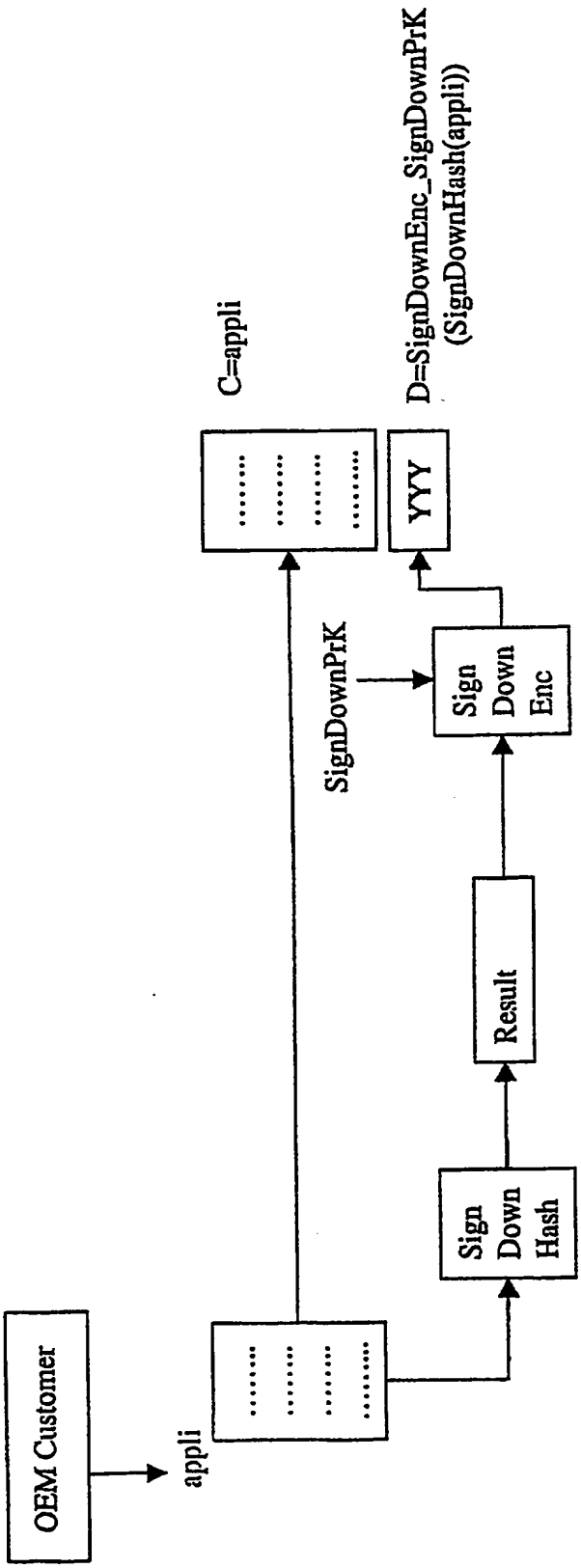

OEM Customer
appli
Sign Down Hash
Result
SignDownPrK
Sign Down Enc
C=appli
D=SignDownEnc_SignDownPrK (SignDownHash(appli))
YYY

Figure 2B

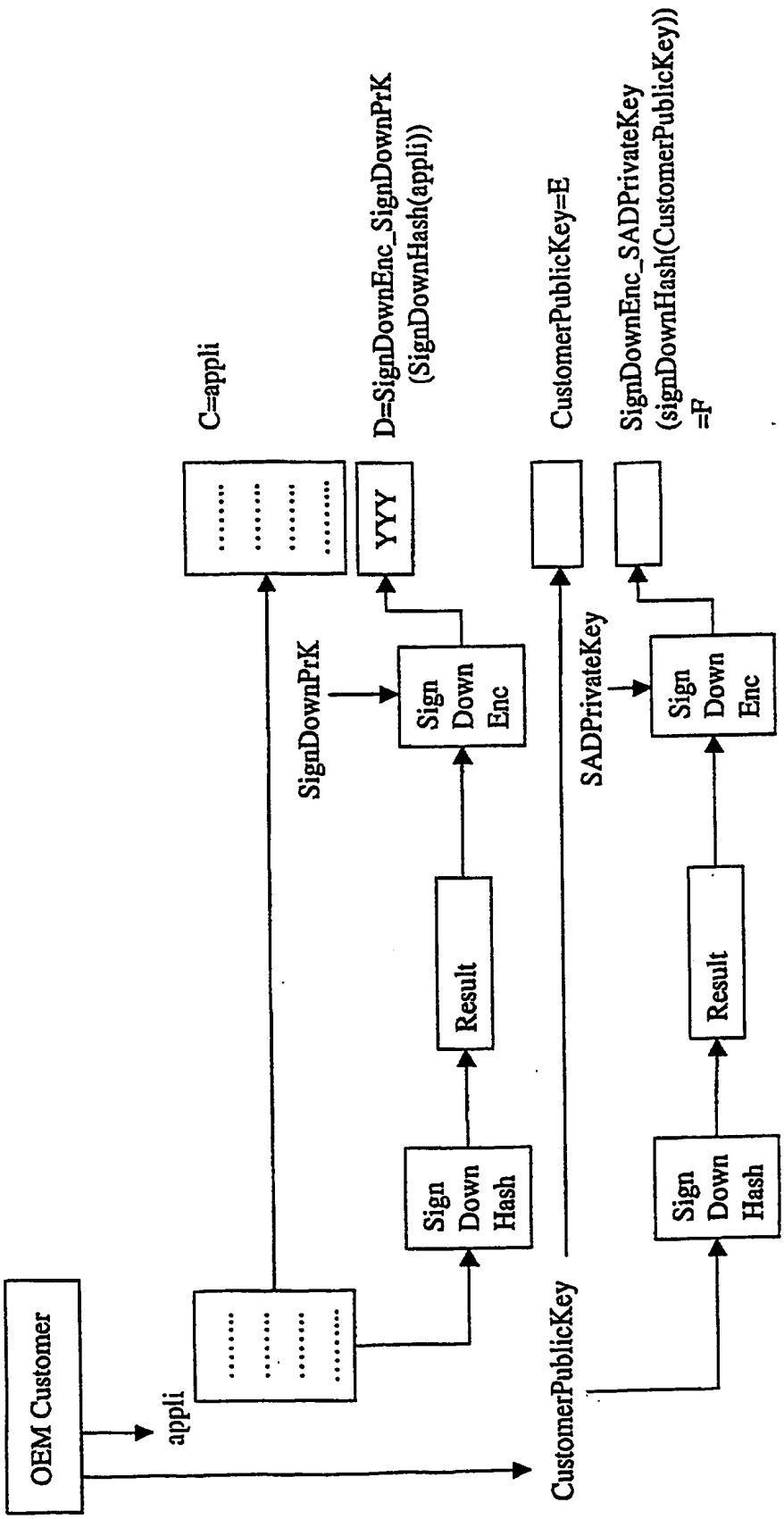

OEM Customer
appli
CustomerPublicKey
Sign Down Hash
Result
Sign Down Enc
SignDownPrK
C=appli
D=SignDownEnc_SignDownPrK (SignDownHash(appli))
YYY
CustomerPublicKey=E
SADPrivateKey
Sign Down Hash
Result
Sign Down Enc
SignDownEnc_SADPrivateKey (signDownHash(CustomerPublicKey)) =F

figure 3A

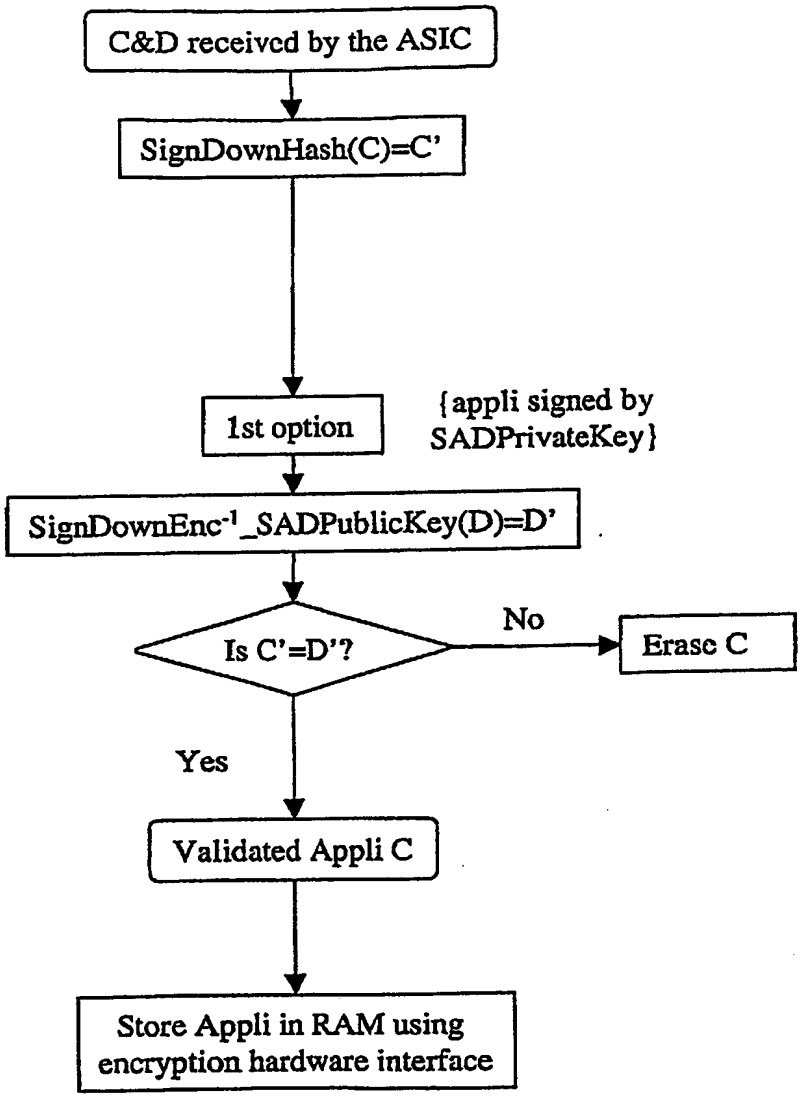

C&D received by the ASIC
SignDownHash(C)=C'
1st option
{appli signed by SADPrivateKey}
SignDownEnc-1_SADPublicKey(D)=D'
Is C'=D'?
No
Erase C
Yes
Validated Appli C
Store Appli in RAM using encryption hardware interface

figure 3B

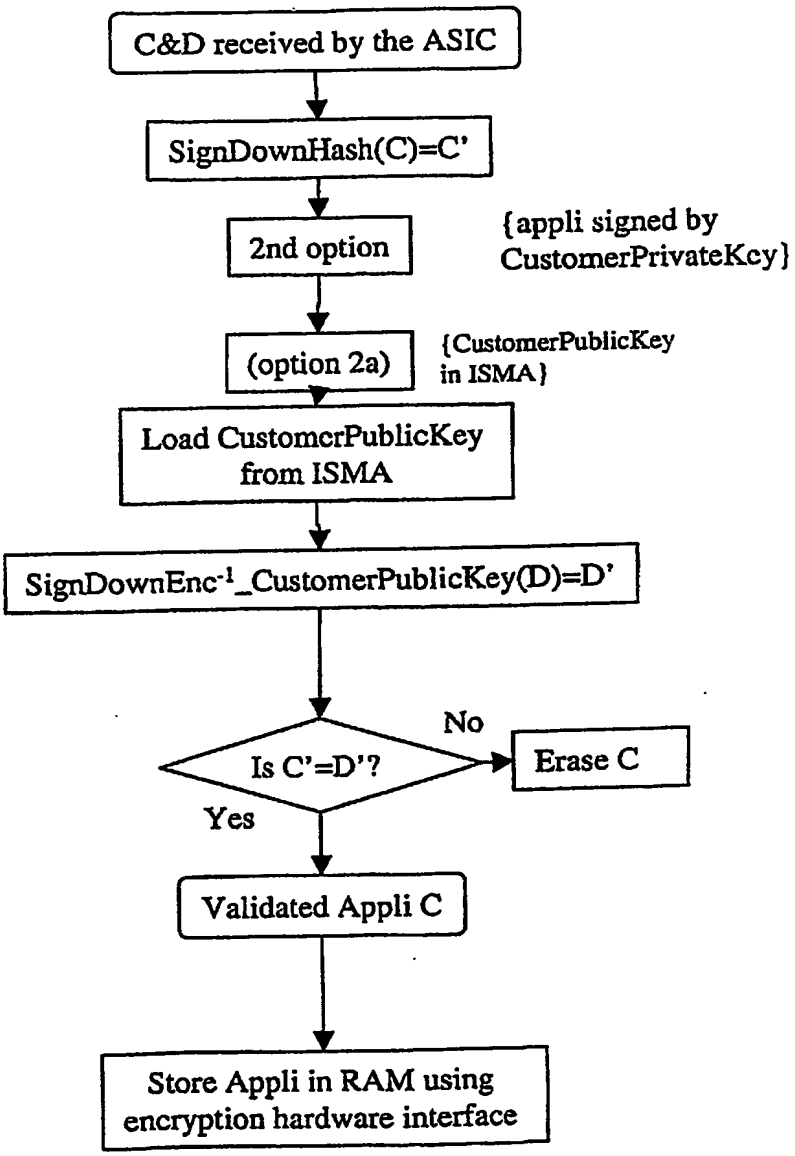

C&D received by the ASIC
SignDownHash(C)=C'
2nd option
{appli signed by CustomerPrivateKey}
(option 2a)
{CustomerPublicKey in ISMA}
Load CustomerPublicKey from ISMA
SignDownEnc-1_CustomerPublicKey(D)=D'
Is C'=D'?
No
Erase C
Yes
Validated Appli C
Store Appli in RAM using encryption hardware interface

Figure 3C

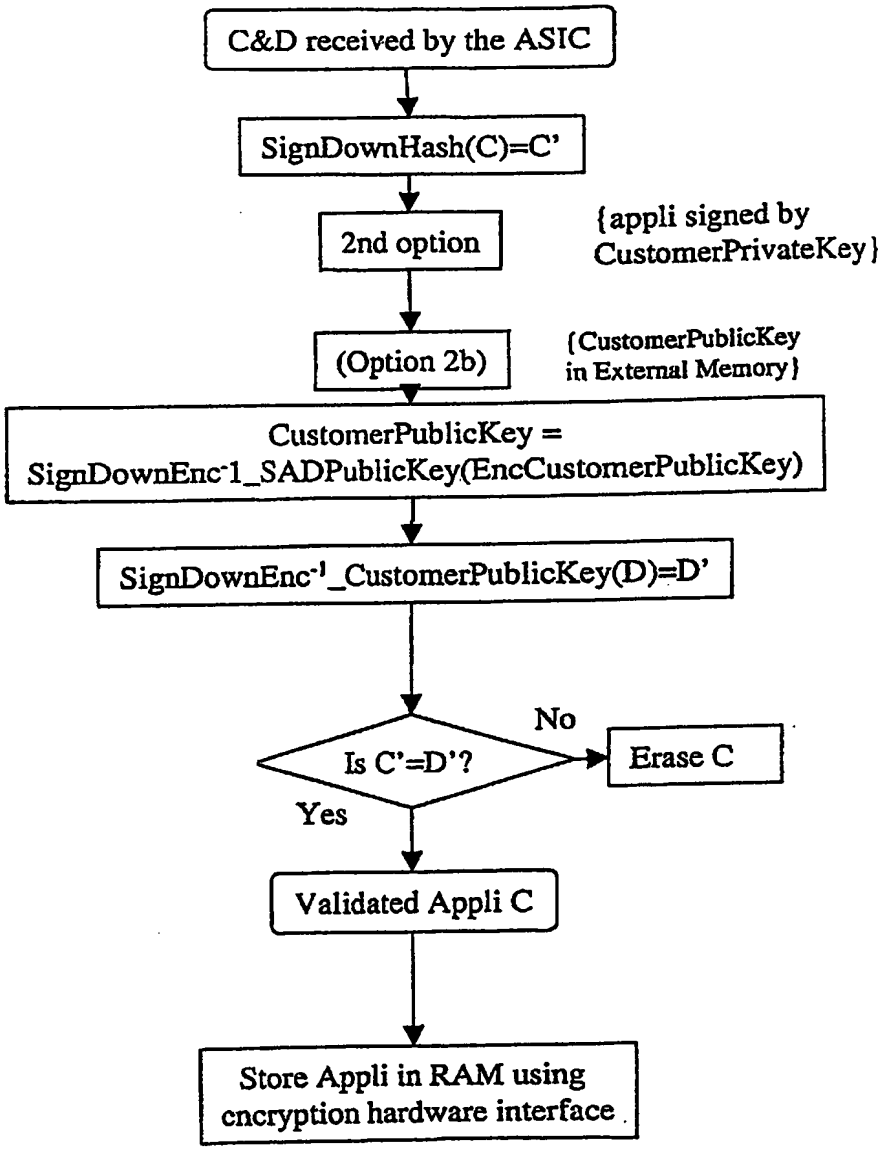

C&D received by the ASIC
SignDownHash(C)=C'
2nd option
{appli signed by CustomerPrivateKey}
(Option 2b)
{CustomerPublicKey in External Memory}
CustomerPublicKey = SignDownEnc-1_SADPublicKey(EncCustomerPublicKey)
SignDownEnc-1_CustomerPublicKey(D)=D'
Is C'=D'?
No
Erase C
Yes
Validated Appli C
Store Appli in RAM using encryption hardware interface

Figure 3D

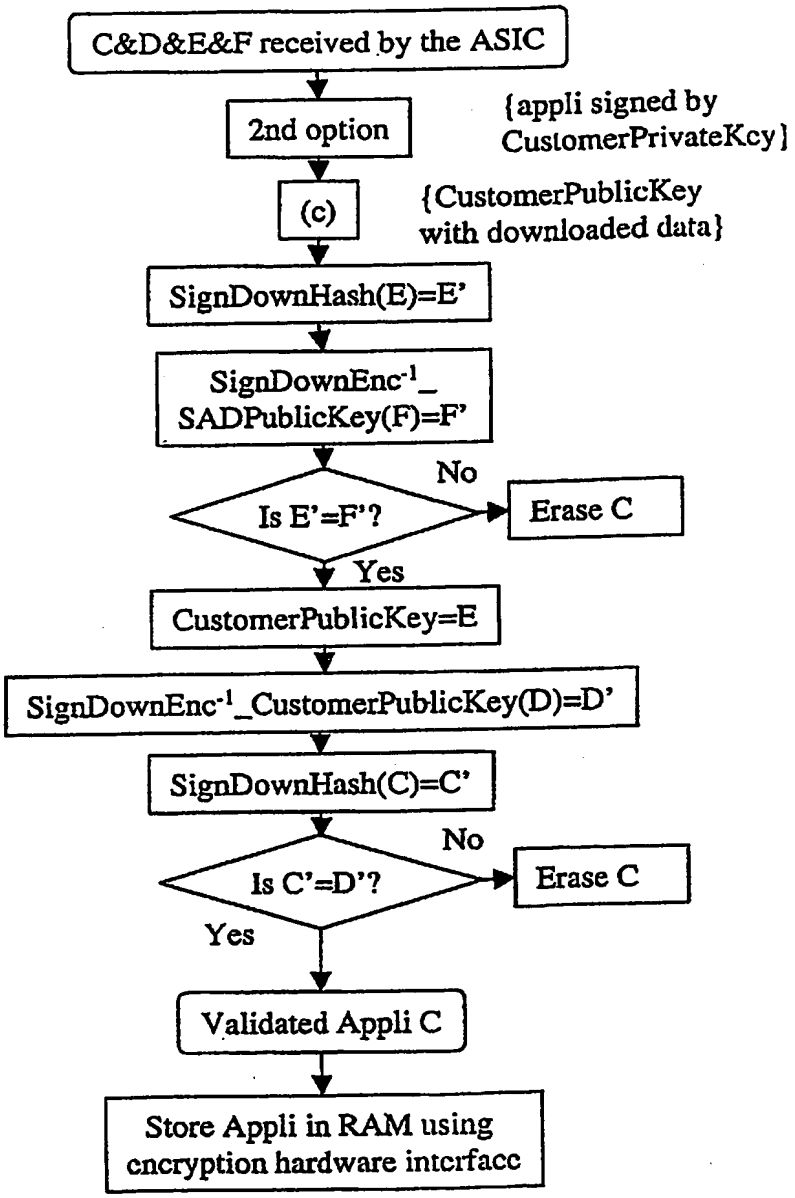

C&D&E&F received by the ASIC
2nd option
{appli signed by CustomerPrivateKey}
(c)
{CustomerPublicKey with downloaded data}
SignDownHash(E)=E'
SignDownEnc-1_ SADPublicKey(F)=F'
No
Is E'=F'?
Erase C
Yes
CustomerPublicKey=E
SignDownEnc-1_CustomerPublicKey(D)=D'
SignDownHash(C)=C'
No
Is C'=D'?
Erase C
Yes
Validated Appli C
Store Appli in RAM using encryption hardware interface

Figure 4A

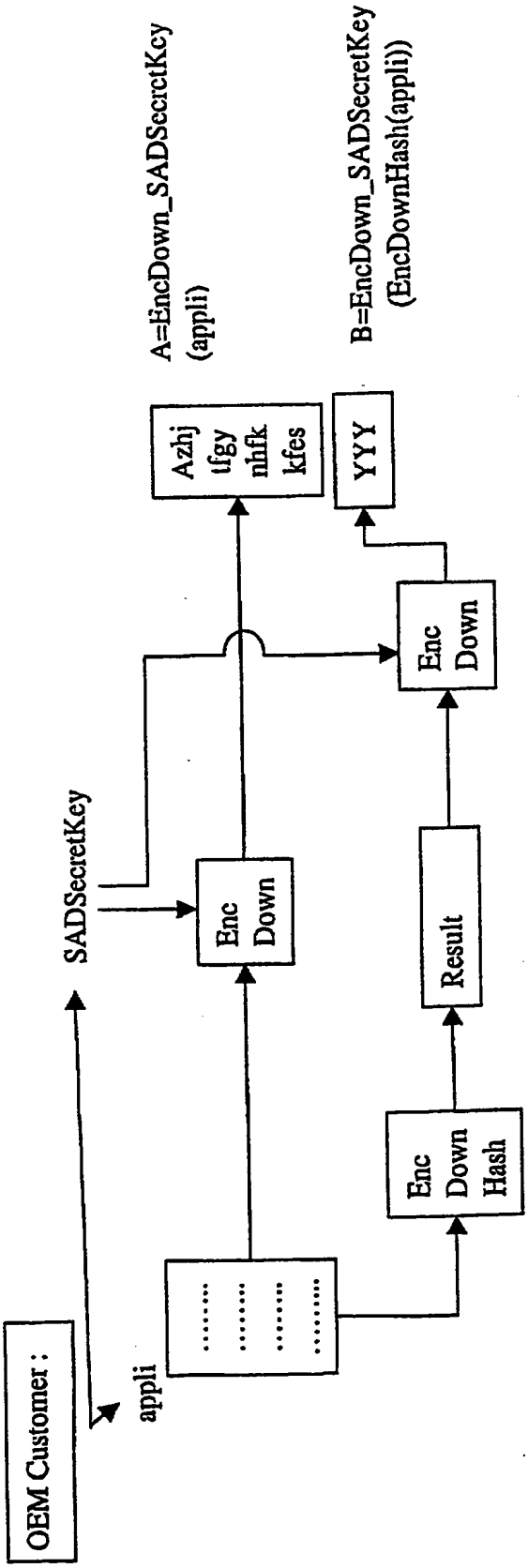

A=EncDown_SADSecretKey
(appli)
B=EncDown_SADSecretKey
(EncDownHash(appli))
Azhj
tfgy
nhfk
kfes
YYY
Enc
Down
Enc
Down
Result
Enc
Down
Hash
SADSecretKey
appli
OEM Customer :

Figure 4B

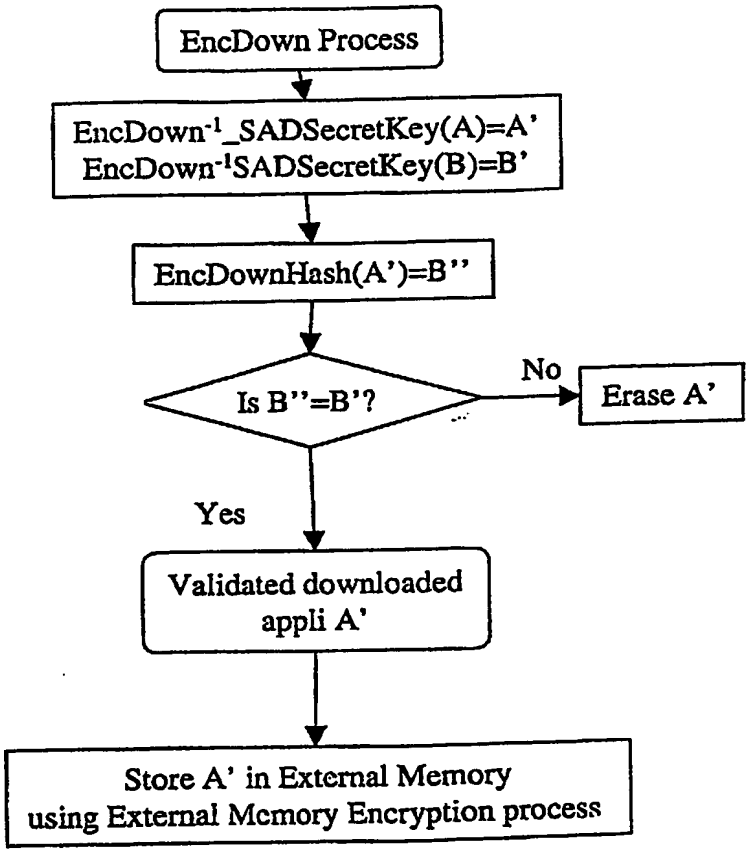

EncDown Process
EncDown-1_SADSecretKey(A)=A'
EncDown-1SADSecretKey(B)=B'
EncDownHash(A')=B''
Is B''=B'?
No
Erase A'
Yes
Validated downloaded appli A'
Store A' in External Memory using External Memory Encryption process

figure 5A

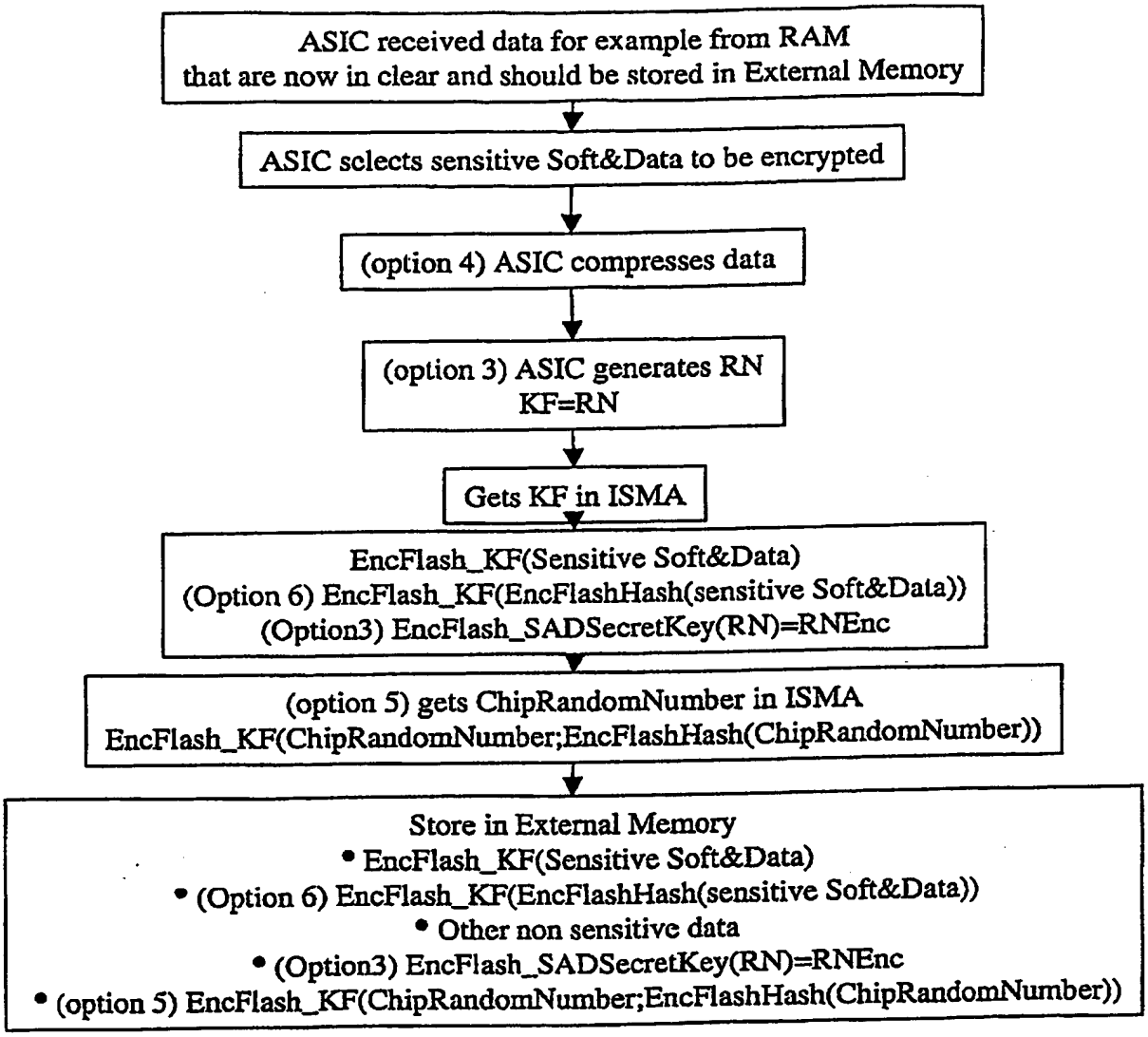

ASIC received data for example from RAM
that are now in clear and should be stored in External Memory
ASIC sclects sensitive Soft&Data to be encrypted
(option 4) ASIC compresses data
(option 3) ASIC generates RN
KF=RN
Gets KF in ISMA
EncFlash_KF(Sensitive Soft&Data)
(Option 6) EncFlash_KF(EncFlashHash(sensitive Soft&Data))
(Option3) EncFlash_SADSecretKey(RN)=RNEnc
(option 5) gets ChipRandomNumber in ISMA
EncFlash_KF(ChipRandomNumber;EncFlashHash(ChipRandomNumber))
Store in External Memory
• EncFlash_KF(Sensitive Soft&Data)
• (Option 6) EncFlash_KF(EncFlashHash(sensitive Soft&Data))
• Other non sensitive data
• (Option3) EncFlash_SADSecretKey(RN)=RNEnc
• (option 5) EncFlash_KF(ChipRandomNumber;EncFlashHash(ChipRandomNumber))

figure 5B

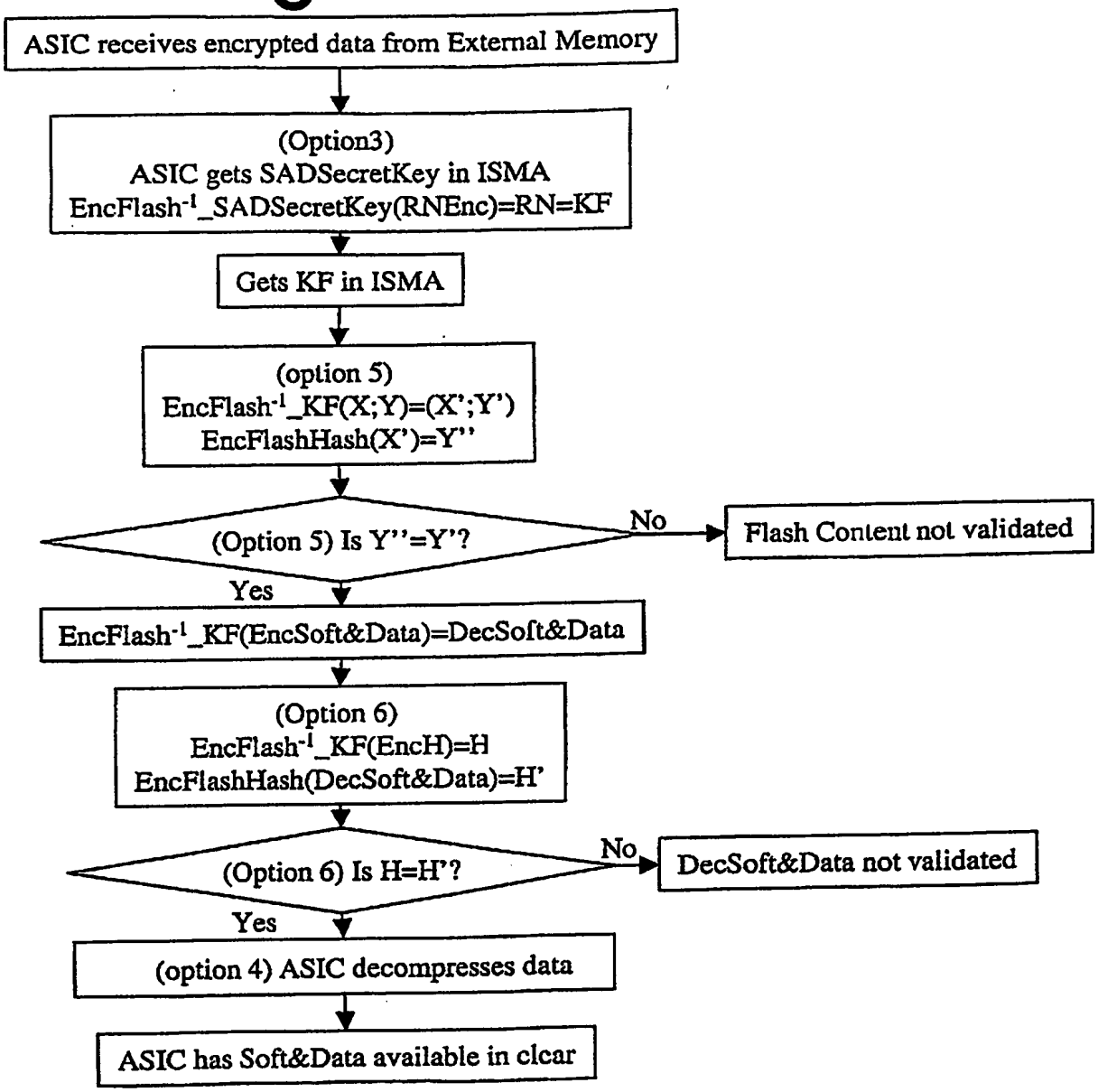

ASIC receives encrypted data from External Memory
(Option3)
ASIC gets SADSecretKey in ISMA
EncFlash-1_SADSecretKey(RNEnc)=RN=KF
Gets KF in ISMA
(option 5)
EncFlash-1_KF(X;Y)=(X';Y')
EncFlashHash(X')=Y''
(Option 5) Is Y''=Y'?
No
Flash Content not validated
Yes
EncFlash-1_KF(EncSoft&Data)=DecSoft&Data
(Option 6)
EncFlash-1_KF(EncH)=H
EncFlashHash(DecSoft&Data)=H'
(Option 6) Is H=H'?
No
DecSoft&Data not validated
Yes
(option 4) ASIC decompresses data
ASIC has Soft&Data available in clear

figure 6

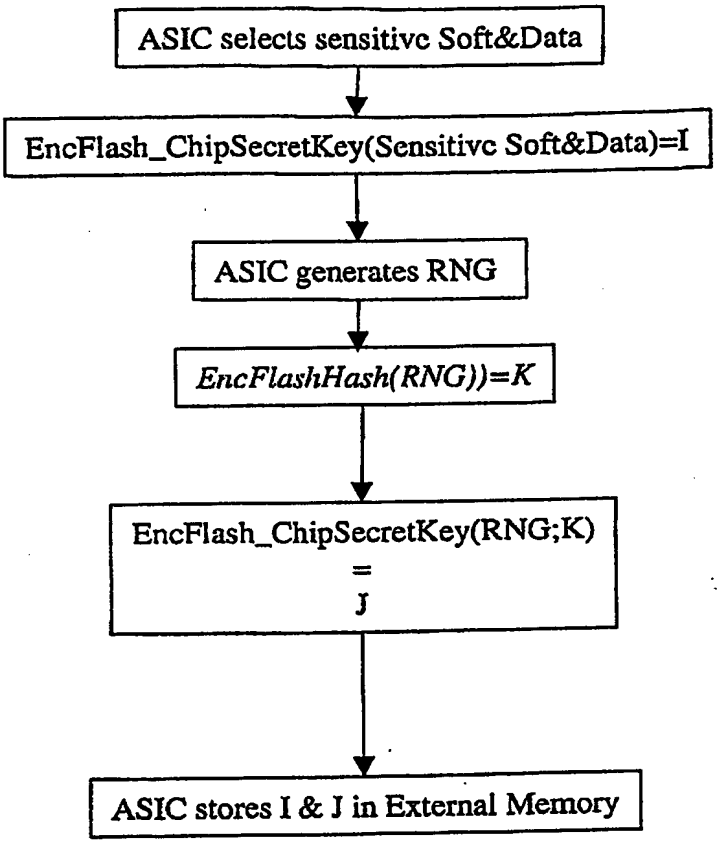

ASIC selects sensitive Soft&Data
EncFlash_ChipSecretKey(Sensitive Soft&Data)=I
ASIC generates RNG
EncFlashHash(RNG))=K
EncFlash_ChipSecretKey(RNG;K)
=
J
ASIC stores I & J in External Memory

figure 7

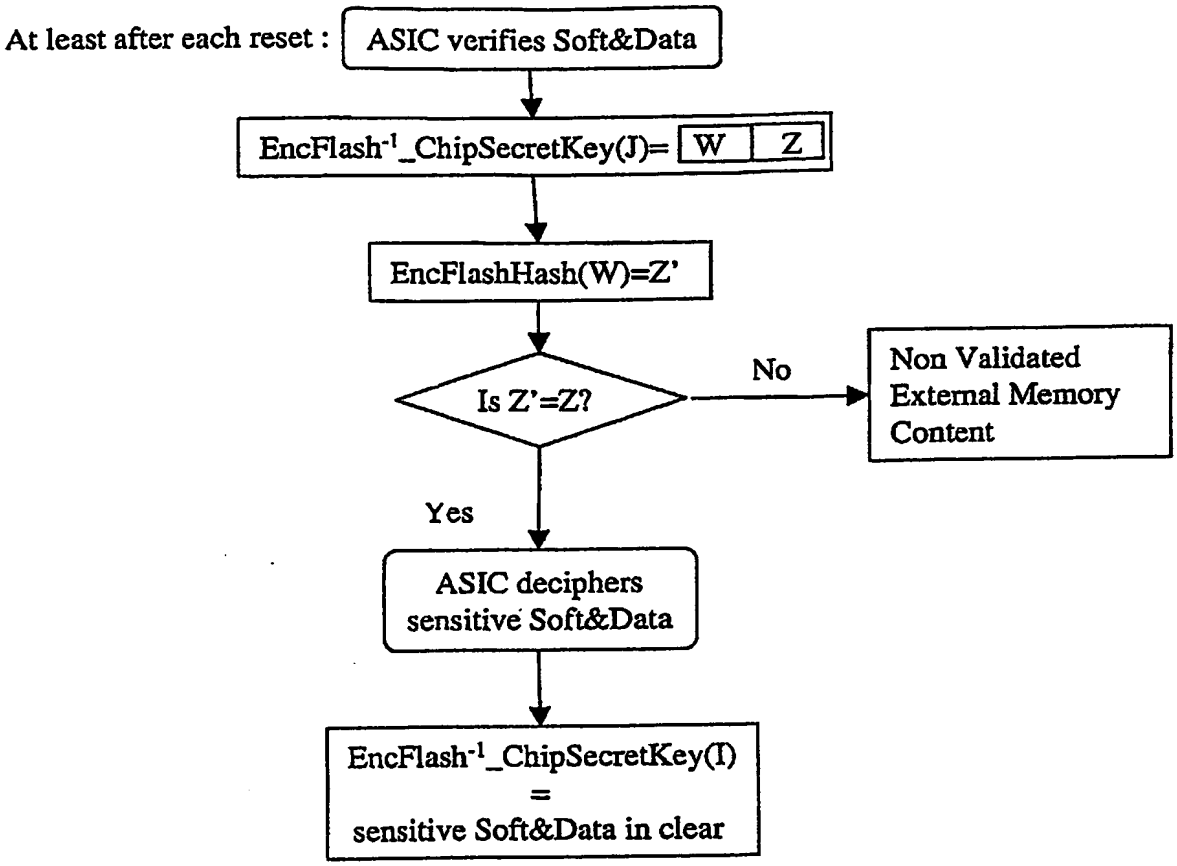
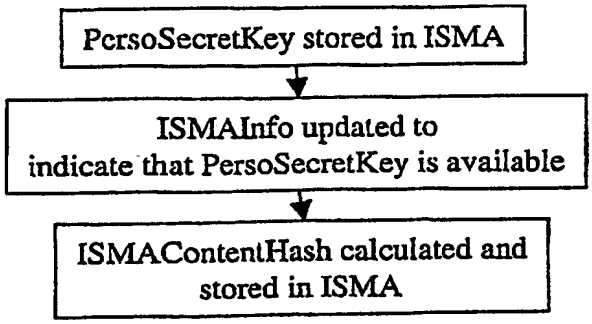

At least after each reset :
ASIC verifies Soft&Data
EncFlash-1_ChipSecretKey(J)= W Z
EncFlashHash(W)=Z'
Is Z'=Z?
No
Non Validated External Memory Content
Yes
ASIC deciphers sensitive Soft&Data
EncFlash-1_ChipSecretKey(I) = sensitive Soft&Data in clear

figure 8



ISMA after First level personalization

ASIC ISMA :

	f PersoSecretKey *f ISMAInfo* *f ISMAContentHash*

figure 9

SAD provides personalization application PersoAppli to OEM customer

EncPers_PersoSecretKey(PersoAppli) & SignPersEnc_SADPrivateKey(SignPersHash(PersoAppli)) or EncPers_PersoSecretKey(PersoAppli;SignPersEnc_SADPrivateKey(SignPers Hash(PersoAppli)) downloaded by OEM customer

PersoAppli is available in a protected and signed format OEM Customer's ASIC having PersoSecretKey & SADPublicKey will be able to authenticate it, and then to unencrypt it.

- SignPersHash is a hash function used to give a 20 Bytes result relevant to PersoAppli integrity
- SignPersEnc is an encryption (signature)algorithm used to encrypt the hash result asymmetrically with SADPrivateKey
- EncPers is an encryption symmetric tool used to encrypt the personalization software and eventually its signature

ISMA after Second level personalization

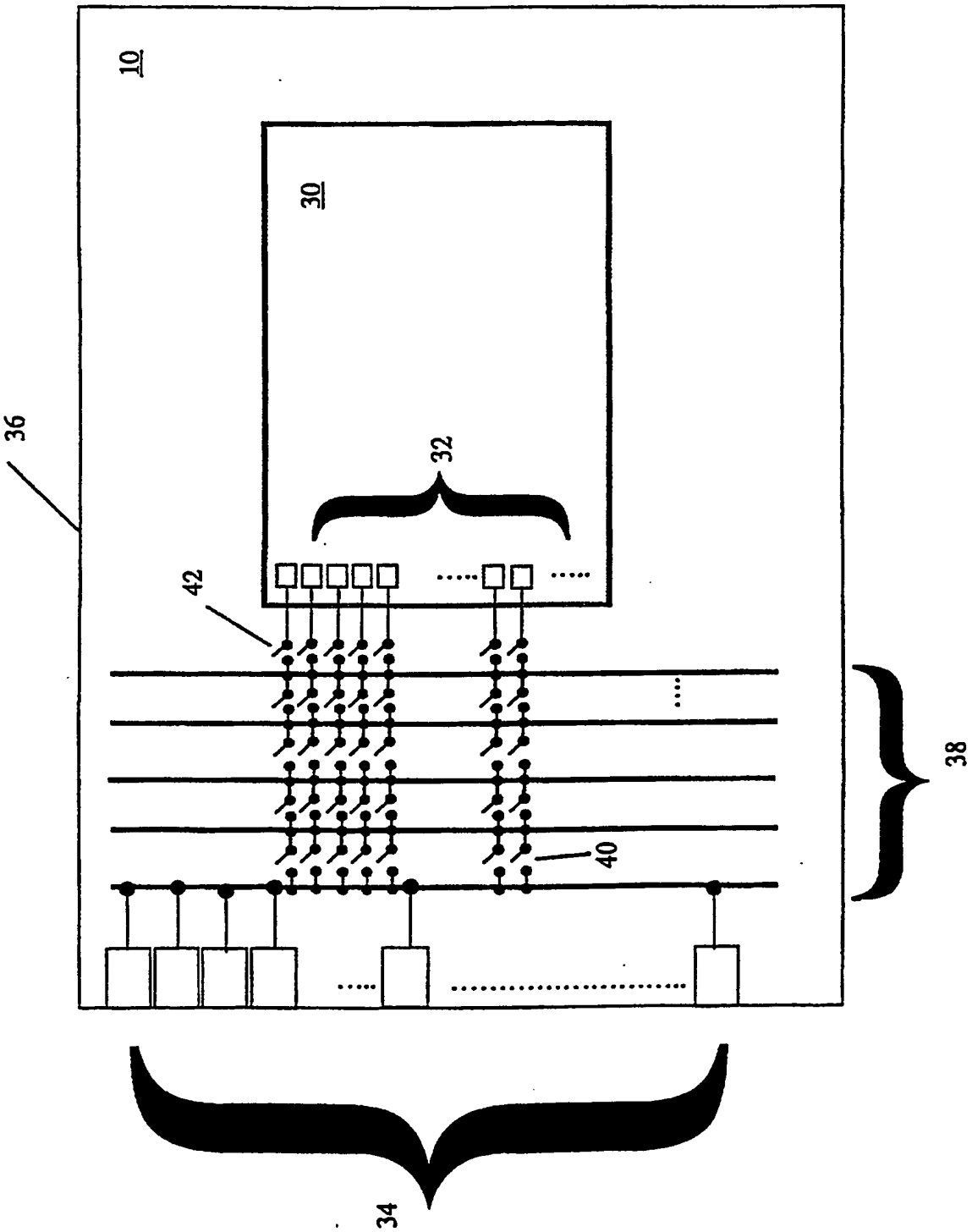
ASIC ISMA :

	f Sensitive data *f ISMAInfo* *f ISMAContentHash*

PersoAppli will have the task
- to file ISMA with sensitive data
- erase PersoSecretKey
- update ISMAInfo
- Compute and write ISMAContentHash
- erase PersoAppli

PersoAppli will stored sensitive data corresponding to the different option corresponding to the OEM customer requirements. It could be run directly or stored in the External Memory using EncFlash_PersoSecretKey (means KF = PersoSecretKey).

figure 10



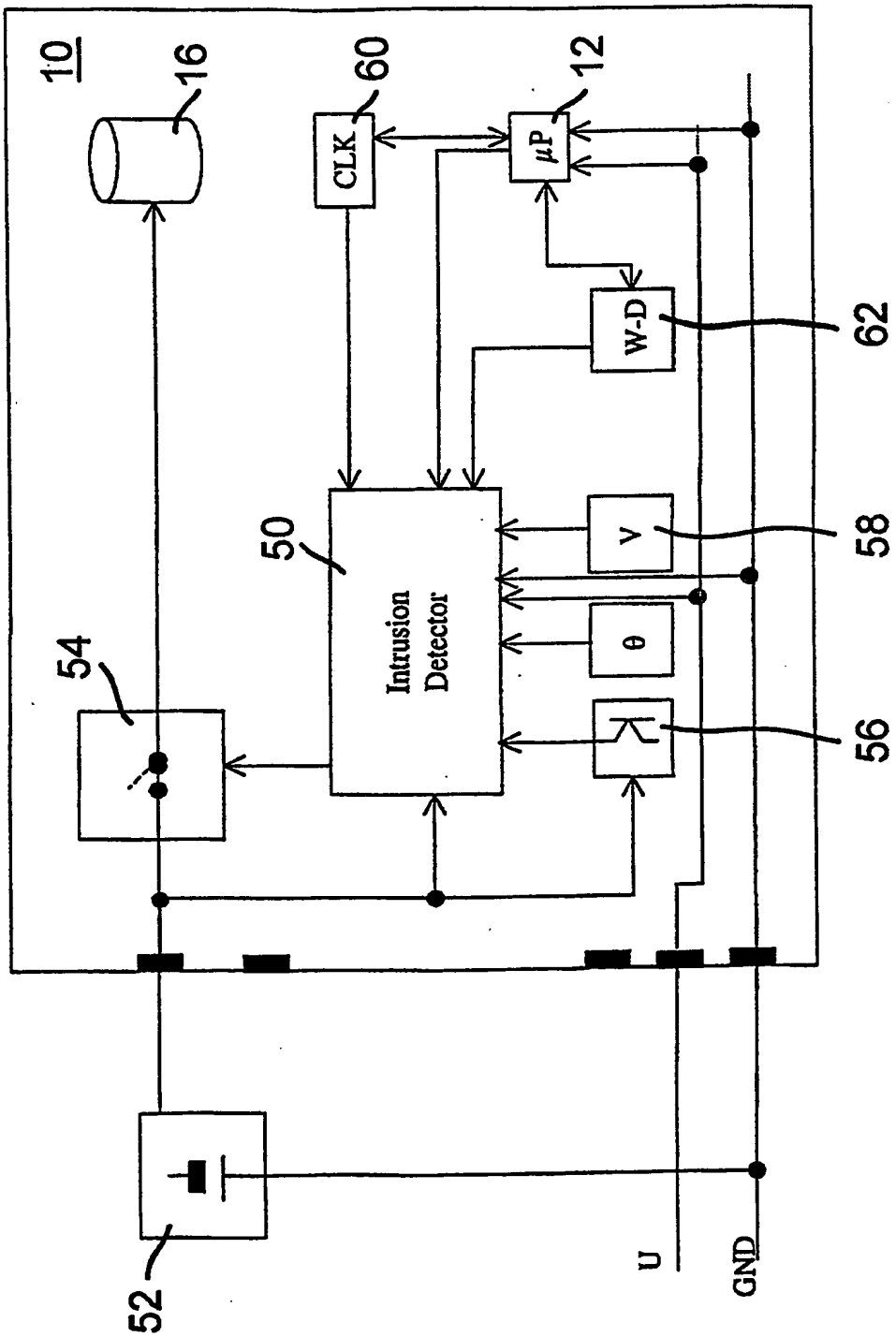

10
16
60
12
CLK
μP
W-D
62
50
Intrusion Detector
V
58
θ
54
56
52
U
GND

figure 11

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

10/500983

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number
WO 2003/058409 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/EP2003/000075

(22) International Filing Date: 7 January 2003 (07.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 00 288.6 7 January 2002 (07.01.2002) DE

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS GMBH** [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRESSY, Philippe** [FR/FR]; 8, rue du Lancon, F-83190 Ollioules (FR). **LOISEL, Yann** [FR/FR]; Lotissement Le Revestin, Chemin des Severiers, F-13600 La Ciotat (FR).

(74) Agent: **DEGWERT, Hartmut**; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

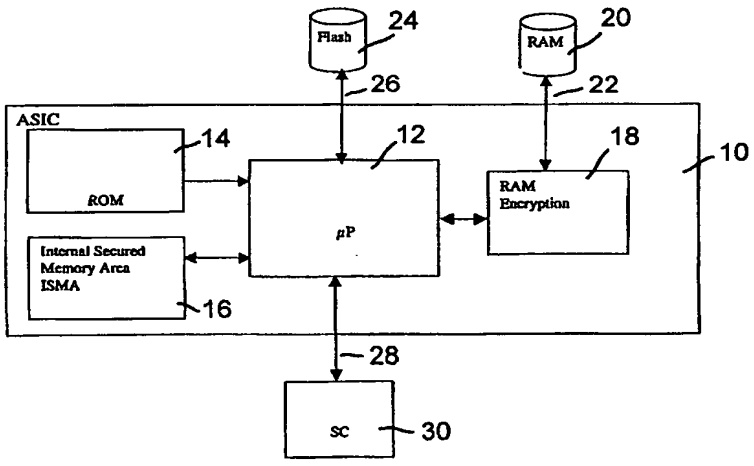
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 June 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTECTING A DEVICE AGAINST UNINTENDED USE IN A SECURE ENVIRONMENT



(57) Abstract: A method and device are disclosed for executing applications that involve secure transactions and/or conditional access to valuable contents and/or services. The device includes an integrated circuit that has a central processing unit, an internal memory, input/output connections for external memory and connection ports for an external interface circuit incorporated on a single chip. The internal memory includes a secured memory area accessible to the central processing unit only. The secret memory area contains a secret encryption key used for encryption of sensitive data stored in the external memory. Preferably, the chip includes a random number generator. A hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with the secret key, and the encrypted random number with its hash value are stored in the external memory. As a result, the device has a chip that is uniquely paired with the external memory.

WO 2003/058409 A3

INTERNATIONAL SEARCH REPORT

Inter [redacted] Application No
PCT/[redacted]3/00075

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

PAJ, WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/19299 A (HUGHES ELECTRONICS CORP) 6 April 2000 (2000-04-06)	1,9,17, 18, 20-22, 26-37
Y	page 1, line 18 -page 2, line 1 page 5, line 15 -page 6, line 3 page 8, line 1 - line 14 page 12, line 10 -page 13, line 6 page 21, line 7 - line 10 page 33, line 11 - line 12 page 40, line 6 - line 7 page 47, line 9 - line 10 page 70, line 6 - line 20 page 74, line 14 - line 15 figures 1-3	3-8, 23-25

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 2004	07/05/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

INTERNATIONAL SEARCH REPORT

Inter[redacted] Application No
PCT/[redacted]3/00075

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 168 172 A (FUJITSU LTD) 2 January 2002 (2002-01-02) column 1, paragraphs 2-5 column 10, paragraph 42 column 12, paragraph 56 -column 16, paragraph 82 figure 1	1,3-9, 17,20-28
X	US 6 061 449 A (SPRUNK ERIC ET AL) 9 May 2000 (2000-05-09) column 1, line 18,25-28 column 5, line 44 - line 50 column 8, line 46 - line 50 column 9, line 48 - line 51 column 12, line 13 - line 27 column 17, line 60 -column 25, line 19 column 26, last line -column 27, line 5 column 28, line 48 - line 51 figure 1	1,3-9, 17,18, 20-32
Y	US 2001/018745 A1 (LACZKO FRANK L ET AL) 30 August 2001 (2001-08-30) page 2, paragraphs 21,26 page 4, paragraph 37 page 5, paragraph 44 page 6, paragraph 49 figure 1	3-8, 23-25

INTERNATIONAL SEARCH REPORT

[redacted] on patent family members

Inter [redacted] Application No
PCT/[redacted]03/00075

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0019299 A	06-04-2000	WO 0019299 A1	06-04-2000
		AU 743775 B2	07-02-2002
		AU 1062399 A	17-04-2000
		CA 2309627 A1	06-04-2000
		EP 1032869 A1	06-09-2000
		JP 2002526822 T	20-08-2002
EP 1168172 A	02-01-2002	JP 2002014871 A	18-01-2002
		EP 1168172 A2	02-01-2002
		US 2002002676 A1	03-01-2002
US 6061449 A	09-05-2000	CA 2249554 A1	10-04-1999
		CN 1236132 A	24-11-1999
		EP 0908810 A2	14-04-1999
		IL 126448 A	14-08-2002
		TW 445402 B	11-07-2001
US 2001018745 A1	30-08-2001	US 6266754 B1	24-07-2001
		EP 0961193 A2	01-12-1999
		JP 2000138917 A	16-05-2000